House Judiciary Committee
Representative William Van Regenmorter
May 3, 2006

Representative Van Regenmorter and Committee Members:

Thank you for allowing me to speak on behalf of Senator Brown to SB 53, 54, and 151. I am Jeanne Laimon, Legislative Director, Office of Senator Cameron Brown.

Senate Bills 53, 54 and 151 were unanimously voted out of the Senate Committee on Technology and Energy on February 16, 2005 and voted out of the Senate unanimously (w/one excused) on March 9, 2005. This legislation would protect consumers from "spyware," which can monitor Web-based information and prompt pop-up advertisements.

Consumers often unknowingly agree to download spyware systems when they accept software licensing agreements while downloading software from the Internet. Deceptively installed spyware can hurt the performance and stability of computer systems and may even cause computers to crash. A survey conducted by Internet service provider America Online found that 80 percent of home computers are infected with some form of spyware.

When someone logs on to a personal computer, there is a reasonable assumption that their transactions will be made safely and privately, but this is often not the case. One's right to privacy shouldn't be violated in one's own home or in one's own home computer.

With Senator Brown's legislation, violators would be subject to either a misdemeanor or felony charge, depending on the severity of the violation, punishable by a fine of up to $10,000 or imprisonment for 93 days to four years.

Federal law makers are currently advancing similar legislation in the United States Congress. (H.R. 29 – US Rep Mary Bono).

When this package of spyware legislation was in the Senate Tech and Energy Committee, several concerns were raised by various parties such as law enforcement, prosecutors, Attorney General's office and the Internet industry groups. Many of these concerns have been addressed in the substitute bills that passed the Senate and Senator Brown has expressed his willingness to address any further concerns if necessary.

Some of the concerns raised:

Attorney General's office expressed concern about the volume of spyware violations that occur and its limited resources to pursue violators. There is a general concern that this legislation may create an unreasonable expectation that the Attorney General's office will be able to pursue each violation. To attempt to address this concern, SB 151 S-2 creates a private right of action so harmed users can pursue claims on their own behalf.

(Note: SB 151 S-2 authorizes the Attorney General's Office, which has a call center that already takes computer-related complaints, to file an action against a person for violating this Act. Additionally, Section 6 of the SB 151 (S-2) delineates who else may bring an action under the law and includes: a) a user, b) an Internet Web site owner or registrant, c) a trademark or copyright owner, or d) an authorized advertiser on an Internet Web site).

Industry participants expressed strong concern about there being a private right of action in the bill, the concern being that it (Industry) will be unnecessarily subjected to numerous nuisance suits as a result of this legislation. To assuage Industry, several provisions were added to SB 151 S-2, including making the burden of proof higher by including knowledge and intent components, adding "a loser pays" provision, and the inclusion of the prohibition on class actions. It is my understanding that Industry still may have concerns regarding the private right of action provision.

In summarizing, once installed, spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers. Spyware creates serious electronic privacy concerns and has been the focus of legislation on both the state and federal levels. Senator Brown's legislation (SB 151 S-2) creates civil liability and remedies for the unauthorized installation of spyware onto another person's computer and (SB 53-54) makes it unlawful to install or attempt to install "spyware" into a computer program, computer, computer system, or computer network unless specific conditions are met. Spyware is generally defined as any software that covertly gathers user information or installs advertisements into a computer through the user's Internet connection without his or her knowledge.

Thank you!

***

RECAP:

Major issue:

-80% of computers are infected with spyware (estimated)
-In addition to creating a nuisance and compromising the security of personal information, spyware can interfere with a computer's performance, i.e. sluggish performance, increased pop-up ads, unexplained homepage changes, system crashes
-Once installed, spyware can be extremely difficult to remove

Before spyware legislation moved out of Senate Tech and Energy Committee:
Meetings were held with industry folks: Thursday, Feb. 26' 2005
Friday, March 4, 2005

Over 15 representatives from industry (Microsoft, Yahoo, Michigan Cable, Comcast, Verizon, SBC, CE, DTE, etc.) along with representatives from the Attorney General's office and State Police met with Sen. Brown's staff, Sen. Patterson's staff, and Senate Majority Policy Office staff on two separate occasions to discuss concerns regarding spyware legislation.

Senator Brown has been very open and has taken into consideration several of the concerns brought to his attention. He has tried to incorporate the suggested changes, including definition-tightening. The major issue with industry was with (SB 151): industry either wanted the language "intentionally deceptive" used throughout the bill or wanted ***private right of action*** removed from the bill. Senator Brown added to the definition of "deceptively" to include "intent" element. Private right of action remains in the bill (SB 151).

***